

On Approximate Diagnosability of Nonlinear Systems

Elena De Santis, Giordano Pola and Maria Domenica Di Benedetto

Abstract—This paper deals with diagnosability of discrete-time nonlinear systems with unknown inputs and quantized outputs. We propose a novel notion of diagnosability that we term *approximate diagnosability*, corresponding to the possibility of detecting within a finite delay and *within a given accuracy* if a set of faulty states is reached or not. Addressing diagnosability in an approximate sense is primarily motivated by the fact that system outputs in concrete applications are measured by sensors that introduce measurement errors. Consequently, it is not possible to detect exactly if the state of the system has reached or not the set of faulty states. In order to check approximate diagnosability on the class of nonlinear systems we use tools from formal methods. We first derive a symbolic model approximating the original system within any desired accuracy. This step allows us to check approximate diagnosability of the symbolic model. We then establish the relation between approximate diagnosability of the symbolic model and of the original nonlinear system.

keywords: approximate diagnosability, nonlinear systems, quantized systems, symbolic models.

I. INTRODUCTION

The increasing complexity in real-world engineered systems requires great attention to performance degradation, safety hazards and occurrence of faults, which must be detected as soon as possible to possibly restore nominal behavior of the system. The notion of diagnosability plays a key role in this regard, since it corresponds to the possibility of detecting within a finite delay if a fault, or in general a hazardous situation, occurred. This notion has been extensively studied both in the Discrete-Event Systems (DES) community and control systems community, and the related literature is very broad. Within the DES community, after the seminal work [1], several results have been achieved, see e.g. [2], [3], [4], [5], [6], [7], [8], [9] and the references therein. An excellent review of recent advances on diagnosis methods can be found in [10]. More recently, a unifying framework for the study of observability and diagnosability of DES has been also proposed in [11]. Within the control systems community, for fault-tolerant control, an early review paper was presented in [12], which introduced the basic concepts of fault-tolerant control and analyzed the applicability of artificial intelligence to fault-tolerant control systems. Subsequent overviews appeared in [13], [14]. Reconfigurable fault-tolerant control systems are reviewed in [15], [16], [17] and some results on fault-tolerant control for nonlinear systems

in [18]. A recent comprehensive survey on diagnosability of continuous systems is reported in [19]. Extensions to hybrid systems, featuring both discrete and continuous dynamics, are also present in the literature. For example, [20] addressed diagnosability for timed automata, [21] diagnosability for hybrid systems, [22], [23], [24] propose abstraction techniques for diagnosability of hybrid automata. Apart from differences in the class of systems considered and in the way faults are modeled, to the best of our knowledge, existing papers, except for [25], [26], *either assume that state variables are available, or assume the exact knowledge of output variables*. This is rather limiting in concrete applications where state variables cannot be directly measured, or output variables are measured by sensors that introduce measurement errors. The papers [25] and [26] study diagnosability for quantized systems. They both model faults as additional inputs to the system. The former considers continuous-time nonlinear systems and the detection is done in a stochastic setting, by assuming an appropriate description of the occurrence of faults. The latter analyzes discrete-time linear systems and the faults are detected, provided that they belongs to an appropriate class of functions.

In this paper, we introduce a new notion of diagnosability, that we term *approximate diagnosability*, for discrete-time nonlinear systems with unknown inputs and quantized output measurements. Given an accuracy $\rho \geq 0$ and a set of faulty states \mathcal{F} , approximate diagnosability corresponds to the possibility of detecting, within a finite time delay:

- if the system's state reached the set $\mathcal{F} + \mathcal{B}_\rho(0)$, obtained by adding to \mathcal{F} a closed ball $\mathcal{B}_\rho(0)$ centered at the origin and with radius ρ , and
- if the system's state has never reached the set \mathcal{F} .

This ambiguity around the set \mathcal{F} reflects uncertainties introduced by measurement errors. When the accuracy $\rho = 0$, approximate diagnosability translates to dynamical systems the notion of diagnosability investigated in [11] for DES.

In order to check this property on the class of nonlinear systems we use tools from formal methods. Under an assumption of incremental stability of the nonlinear system we first derive a symbolic model approximating the original system within any desired accuracy. We recall that a symbolic model is an abstract description of the control system where each state corresponds to an aggregate of continuous states and each control label corresponds to an aggregate of continuous inputs. We then extend the classical notion of diagnosability given for DES to metric symbolic models and in an approximate sense. Algorithms for checking this property can be easily obtained by naturally extending those

The authors are with the Department of Information Engineering, Computer Science and Mathematics, Center of Excellence DEWS, University of L'Aquila, 67100 L'Aquila, Italy, {elena.desantis,giordano.pola,mariadomenica.dibenedetto}@univaq.it.

This work has been partially supported by the Center of Excellence for Research DEWS, University of L'Aquila, Italy.

proposed in [11] to an approximate sense. We finally show how to check approximate diagnosability of the original nonlinear system by analyzing the same property on the obtained symbolic model. Computational complexity of the proposed approach is also discussed.

This paper is organized as follows. Section II introduces notation and preliminary definitions. Section III introduces the notion of approximate diagnosability for the class of discrete-time nonlinear systems. In Section IV we first derive symbolic models approximating the nonlinear system in the sense of approximate bisimulation, we then extend the notion of diagnosability given for DES to metric symbolic systems and in an approximate sense, and then establish connections between approximate diagnosability of the symbolic model and approximate diagnosability of the original nonlinear system. Some concluding remarks are offered in Section V.

II. NOTATION AND PRELIMINARY DEFINITIONS

The symbols \mathbb{N} , \mathbb{Z} , \mathbb{R} , \mathbb{R}^+ and \mathbb{R}_0^+ denote the set of non-negative integer, integer, real, positive real, and nonnegative real numbers, respectively. The symbol 0_n denotes the origin in \mathbb{R}^n . Given $a, b \in \mathbb{Z}$, we denote $[a; b] = [a, b] \cap \mathbb{Z}$. Given a set X , the symbol 2^X denotes the power set of X . Given a pair of sets X and Y and a relation $\mathcal{R} \subseteq X \times Y$, the symbol \mathcal{R}^{-1} denotes the inverse relation of \mathcal{R} , i.e. $\mathcal{R}^{-1} = \{(y, x) \in Y \times X : (x, y) \in \mathcal{R}\}$. Given $X' \subseteq X$ and $Y' \subseteq Y$, we denote $\mathcal{R}(X') = \{y \in Y | \exists x \in X' \text{ s.t. } (x, y) \in \mathcal{R}\}$ and $\mathcal{R}^{-1}(Y') = \{x \in X | \exists y \in Y' \text{ s.t. } (x, y) \in \mathcal{R}\}$. Given a function $f : X \rightarrow Y$ and $X' \subseteq X$ the symbol $f(X')$ denotes the image of X' through f , i.e. $f(X') = \{y \in Y | \exists x \in X' \text{ s.t. } y = f(x)\}$ and the symbol $f|_{X'}$ denotes the restriction of f to X' that is $f|_{X'} : X' \rightarrow Y$ such that $f|_{X'}(x') = f(x')$ for all $x' \in X'$. A continuous function $\gamma : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$, is said to belong to class \mathcal{K} if it is strictly increasing and $\gamma(0) = 0$; γ is said to belong to class \mathcal{K}_∞ if $\gamma \in \mathcal{K}$ and $\gamma(r) \rightarrow \infty$ as $r \rightarrow \infty$. A continuous function $\beta : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$ is said to belong to class \mathcal{KL} if for each fixed s , the map $\beta(r, s)$ belongs to class \mathcal{K}_∞ with respect to r and, for each fixed r , the map $\beta(r, s)$ is decreasing with respect to s and $\beta(r, s) \rightarrow 0$ as $s \rightarrow \infty$. Symbol I_r denotes the identity matrix in \mathbb{R}^r . Given a vector $x \in \mathbb{R}^n$ we denote by $x(i)$ the i -th element of x and by $\|x\|$ the infinity norm of x . Given $a \in \mathbb{R}$ and $X \subseteq \mathbb{R}^n$, the symbol aX denotes the set $\{y \in \mathbb{R}^n | \exists x \in X \text{ s.t. } y = ax\}$. Given $\theta \in \mathbb{R}^+$ and $x \in \mathbb{R}^n$, we denote

$$\mathcal{B}_\theta(x) = \{y \in \mathbb{R}^n | \|x - y\| \leq \theta\};$$

$$\mathcal{B}_{[-\theta, \theta]}^n(x) = \left\{ \begin{array}{l} y \in \mathbb{R}^n \\ y(i) \in [-\theta + x(i), \theta + x(i)], i \in [1; n] \end{array} \right\}.$$

Note that for any $\theta \in \mathbb{R}^+$, the collection of $\mathcal{B}_{[-\theta, \theta]}^n(x)$ with x ranging in $2\theta\mathbb{Z}^n$ is a partition of \mathbb{R}^n . Given a set $X \subseteq \mathbb{R}^n$ we denote by $\mathcal{B}_\theta(X)$ the set $\bigcup_{x \in X} \mathcal{B}_\theta(x)$. We now define the quantization function.

Definition 1: Given a positive $n \in \mathbb{N}$ and a quantization parameter $\theta \in \mathbb{R}^+$, the quantizer in \mathbb{R}^n with accuracy θ is a function

$$[\cdot]_\theta^n : \mathbb{R}^n \rightarrow 2\theta\mathbb{Z}^n,$$

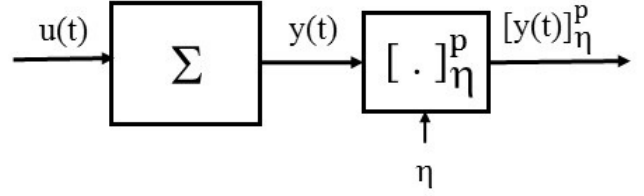


Fig. 1. Nonlinear system with quantized output measurements.

associating to any $x \in \mathbb{R}^n$ the unique vector $[x]_\theta^n \in 2\theta\mathbb{Z}^n$ such that $x \in \mathcal{B}_{[-\theta, \theta]}^n([x]_\theta^n)$.

Definition above naturally extends to sets $X \subseteq \mathbb{R}^n$ when $[X]_\theta^n$ is interpreted as the image of X through function $[\cdot]_\theta^n$.

III. NONLINEAR SYSTEMS AND APPROXIMATE DIAGNOSABILITY

The class of nonlinear systems that we consider in this paper is described by

$$\Sigma : \begin{cases} x(t+1) = f(x(t), u(t)), \\ y(t) = \begin{bmatrix} I_p & 0 \end{bmatrix} x(t), \\ x(0) \in \mathcal{X}_0, x(t) \in \mathbb{R}^n, u(t) \in U, y(t) \in \mathbb{R}^p, t \in \mathbb{N}, \end{cases} \quad (1)$$

where:

- $x(t)$, $u(t)$ and $y(t)$ denote, respectively, the state, the input and the output, at time $t \in \mathbb{N}$;
- \mathbb{R}^n is the state space;
- $\mathcal{X}_0 \subseteq \mathbb{R}^n$ is the set of initial states;
- $U \subseteq \mathbb{R}^m$ is the input set;
- \mathbb{R}^p is the output space with $p < n$;
- $f : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}^n$ is the vector field.

In this paper we make the following:

Assumption 1:

- set \mathcal{X}_0 is compact;
- set U is compact and contains the origin 0_m ;
- function f is continuous in its arguments and satisfies $f(0_n, 0_m) = 0_n$.

We denote by \mathcal{U} the collection of input functions from \mathbb{N} to U . Given $t_f \in \mathbb{N}$, a function

$$x : [0; t_f] \rightarrow \mathbb{R}^n \quad (2)$$

is said to be a *state trajectory* of Σ if $x(0) \in \mathcal{X}_0$ and there exists $u \in \mathcal{U}$ satisfying $x(t+1) = f(x(t), u(t))$, for all $t \in [0; t_f]$. Given $t_f \in \mathbb{N}$, a function $y : [0; t_f] \rightarrow \mathbb{R}^p$ is said to be an *output trajectory* of Σ if there exists a state trajectory $x : [0; t_f] \rightarrow \mathbb{R}^n$ of Σ such that $y(t) = \begin{bmatrix} I_p & 0 \end{bmatrix} x(t)$ for all times $t \in [0; t_f]$. Given $t_f \in \mathbb{N}$, we denote by \mathcal{Y}_{t_f} the collection of output trajectories of Σ with domain $[0; t_f]$.

Remark 1: The choice in the output function in nonlinear system Σ is motivated by many concrete applications where the output variables correspond to a selection of the state variables. However, it is easy to see that there is no loss of generality in considering output function in (1) in the form of $y(t) = Cx(t)$, $t \in \mathbb{N}$, for some matrix $C \in \mathbb{R}^{p \times n}$, instead of $y(t) = \begin{bmatrix} I_p & 0 \end{bmatrix} x(t)$, $t \in \mathbb{N}$. General nonlinear output

functions are not considered in this paper and will be the object of future investigations.

Throughout the paper we will make the following

Assumption 2: Inputs $u(\cdot) \in \mathcal{U}$ of Σ are not known.

Assumption 3: Output $y(t)$ of Σ at time $t \in \mathbb{N}$ is only available through its quantization $[y(t)]_\eta^p$, where $\eta \in \mathbb{R}^+$ is the quantization parameter, see Fig. 1.

Given the quantization parameter $\eta \in \mathbb{R}^+$ and $t_f \in \mathbb{N}$, we denote by $\mathcal{Y}_{t_f}^\eta$ the collection of quantized output trajectories generated by Σ with domain $[0; t_f]$, i.e. the collection of functions

$$y_{t_f, \eta} : [0; t_f] \rightarrow [\mathbb{R}^p]_\eta^p,$$

such that there exists $y_{t_f} \in \mathcal{Y}_{t_f}$ for which:

$$y_{t_f, \eta}(t) = [y_{t_f}(t)]_\eta^p, \forall t \in [0; t_f].$$

We also set

$$\mathcal{Y}^\eta = \bigcup_{t_f \in \mathbb{N}} \mathcal{Y}_{t_f}^\eta,$$

corresponding to the collection of all quantized output trajectories of Σ . We can now propose the notion of approximate diagnosability for nonlinear systems.

Definition 2: (Approximate diagnosability of nonlinear systems) Given a desired accuracy $\rho \in \mathbb{R}_0^+$ and a set of faulty states $\mathcal{F} \subseteq \mathbb{R}^n$ with

$$\mathcal{F} \cap \mathcal{X}_0 = \emptyset,$$

nonlinear system Σ in (1) is (ρ, \mathcal{F}) -diagnosable if there exists a finite delay $\Delta \in \mathbb{N}$, and

$$\mathcal{D} : \mathcal{Y}^\eta \rightarrow \{0, 1\},$$

called the diagnoser, such that

$$\mathcal{D}(y_{0, \eta}) = 0,$$

and whenever for some time $\mathbf{t} > 0$

$$(x(\mathbf{t}) \in \mathcal{F}) \wedge (x(t) \notin \mathcal{F}, \forall t \in [0; \mathbf{t} - 1])$$

we have

$$\mathcal{D}(y_{\mathbf{t}+\Delta, \eta}) = 1.$$

Conversely, whenever for some time $\mathbf{t}' > 0$

$$(\mathcal{D}(y_{\mathbf{t}', \eta}) = 1) \wedge (\mathcal{D}(y_{t, \eta}) = 0, \forall t \in [0; \mathbf{t}' - 1])$$

we have

$$x(\mathbf{t}) \in \mathcal{B}_\rho(\mathcal{F}),$$

for some $\mathbf{t} \in [\max\{\mathbf{t}' - \Delta, 0\}; \mathbf{t}']$.

Remark 2: Definition above is a natural extension of the notion of diagnosability given in [11] for DES (with finite set of states), along two directions. First, it applies to nonlinear systems, hence dynamical systems with infinite set of states. Second, it is given in an approximate sense. Motivation for addressing approximate diagnosability primarily stems from the fact that outputs of nonlinear systems in concrete applications are measured by sensors that introduce measurement errors. Consequently, it is not possible to detect in general,

with arbitrary small precision if the state of the system is or is not within the set of faulty states. When accuracy $\rho = 0$ definition above coincides with the one of [11], when rewritten for nonlinear systems.

IV. CHECKING APPROXIMATE DIAGNOSABILITY

The approach that we follow to check approximate diagnosability of Σ is based on the use of formal methods and in particular, of symbolic models. Symbolic models are abstract descriptions of control systems where each state corresponds to an aggregate of continuous states and each label to an aggregate of control inputs [27]. This section is organized as follows. In Subsection IV-A we review the notion of systems, approximate relations and extend the notion of diagnosability of [11] to metric symbolic systems and in an approximate sense. In Subsection IV-B we give the main result of the paper: after having approximated the nonlinear system Σ through a symbolic model, we establish connections between approximate diagnosability of the original nonlinear system Σ and approximate diagnosability of the obtained symbolic model; computational complexity of the approach taken is also discussed.

A. Systems, approximate relations and exact diagnosability

We start by recalling the notion of systems that we use to approximate the nonlinear system Σ .

Definition 3: [27] A system is a tuple

$$S = (X, X_0, U, \longrightarrow, Y, H),$$

consisting of

- a set of states X ,
- a set of initial states $X_0 \subseteq X$,
- a set of inputs U ,
- a transition relation $\longrightarrow \subseteq X \times U \times X$,
- a set of outputs Y and,
- an output function $H : X \rightarrow Y$.

A transition $(x, u, x') \in \longrightarrow$ of S is denoted by $x \xrightarrow{u} x'$. The evolution of systems is captured by the notions of state, input and output runs. Given a sequence of transitions of S

$$x_0 \xrightarrow{u_0} x_1 \xrightarrow{u_1} \dots \xrightarrow{u_{l-1}} x_l \quad (3)$$

with $x_0 \in X_0$, the sequences

$$r_X : x_0 x_1 \dots x_l, \quad (4)$$

$$r_U : u_0 u_1 \dots u_{l-1},$$

$$r_Y : H(x_0) H(x_1) \dots H(x_l), \quad (5)$$

are called a *state run*, an *input run* and an *output run* of S , respectively.

The accessible part of a system S , denoted $\text{Ac}(S)$, is the collection of states of S that are reached by state runs of S . System S is said to be:

- *symbolic*, if $\text{Ac}(S)$ and U are finite sets;
- *metric*, if X is equipped with a metric $\mathbf{d} : X \times X \rightarrow \mathbb{R}_0^+$;
- *deterministic*, if for any $x \in X$ and $u \in U$ there exists at most one transition $x \xrightarrow{u} x^+$ and *nondeterministic*, otherwise.

In order to provide approximations of Σ we need to recall the following notions of approximate simulation and bisimulation relations.

Definition 4: [28] Consider a pair of metric systems

$$S_i = (X_i, X_{0,i}, U_i, \xrightarrow{i}, Y_i, H_i), \quad (6)$$

with X_1 and X_2 subsets of some metric set X equipped with metric \mathbf{d} , and let $\varepsilon \in \mathbb{R}_0^+$ be a given accuracy. Consider a relation

$$\mathcal{R} \subseteq X_1 \times X_2 \quad (7)$$

satisfying the following conditions:

- (i) $\forall x_1 \in X_{0,1} \exists x_2 \in X_{0,2}$ such that $(x_1, x_2) \in \mathcal{R}$;
- (ii) $\forall (x_1, x_2) \in \mathcal{R}, \mathbf{d}(x_1, x_2) \leq \varepsilon$.

Relation \mathcal{R} is an ε -approximate (εA) simulation relation from S_1 to S_2 if it enjoys conditions (i)–(ii) and the following one:

- (iii) $\forall (x_1, x_2) \in \mathcal{R}$ if $x_1 \xrightarrow{u_1} x'_1$ then there exists $x_2 \xrightarrow{u_2} x'_2$ such that $(x'_1, x'_2) \in \mathcal{R}$.

System S_1 is ε -simulated by S_2 , if there exists an ε -approximate simulation relation from S_1 to S_2 .

Relation \mathcal{R} in (7) is an ε -approximate (εA) bisimulation relation between S_1 and S_2 if

- \mathcal{R} is an εA simulation relation from S_1 to S_2 , and
- \mathcal{R}^{-1} is an εA simulation relation from S_2 to S_1 .

Systems S_1 and S_2 are ε -bisimilar, denoted $S_1 \cong_\varepsilon S_2$, if there exists an ε -approximate bisimulation relation between S_1 and S_2 .

We conclude this section with the following

Definition 5: (Approximate diagnosability of metric systems) Consider a metric system $S = (X, X_0, U, \xrightarrow{\quad}, Y, H)$, with metric $\widehat{\mathbf{d}}$, and a set $\widehat{\mathcal{F}} \subseteq X$ of faulty states with

$$\widehat{\mathcal{F}} \cap X_0 = \emptyset.$$

Denote by \mathbf{X} and \mathbf{Y} the collection of state runs and of output runs of S , respectively. Denote by $\widehat{\mathcal{B}}_{\widehat{\rho}}(\widehat{x})$ the closed ball induced by metric $\widehat{\mathbf{d}}$ centered at $\widehat{x} \in X$ and with radius $\widehat{\rho}$, i.e.

$$\widehat{\mathcal{B}}_{\widehat{\rho}}(\widehat{x}) = \{x \in X \mid \widehat{\mathbf{d}}(x, \widehat{x}) \leq \widehat{\rho}\}.$$

Given $\widehat{X} \subseteq X$, denote by $\widehat{\mathcal{B}}_{\widehat{\rho}}(\widehat{X})$ the set

$$\bigcup_{\widehat{x} \in \widehat{X}} \widehat{\mathcal{B}}_{\widehat{\rho}}(\widehat{x}).$$

Given a desired accuracy $\widehat{\rho} \in \mathbb{R}_0^+$, system S is $(\widehat{\rho}, \widehat{\mathcal{F}})$ -diagnosable if there exists a finite delay $\widehat{\Delta} \in \mathbb{N}$, and

$$\widehat{\mathcal{D}} : \mathbf{Y} \rightarrow \{0, 1\},$$

called the diagnoser, with

$$\widehat{\mathcal{D}}(y_0) = 0,$$

where y_0 is any output run of S with length 1, such that for any state run $x_0 x_1 \dots x_t \in \mathbf{X}$ and corresponding output run $y_0 y_1 \dots y_t \in \mathbf{Y}$ of S , whenever for some $t > 0$

$$(x_t \in \widehat{\mathcal{F}}) \wedge (x_t \notin \widehat{\mathcal{F}}, \forall t \in [0; t-1]),$$

we have

$$\widehat{\mathcal{D}}(y_{t+\widehat{\Delta}}) = 1.$$

Conversely, whenever for some $t' > 0$

$$(\widehat{\mathcal{D}}(y_{t'}) = 1) \wedge (\widehat{\mathcal{D}}(y_t) = 0, \forall t \in [0; t'-1])$$

we have

$$x_t \in \widehat{\mathcal{B}}_{\widehat{\rho}}(\widehat{\mathcal{F}}),$$

for some $t \in [\max\{(t' - \widehat{\Delta}), 0\}; t']$.

Remark 3: Definition above extends the notion of diagnosability of [11], to metric systems in the sense of Definition 3. In [11], diagnosability with accuracy $\widehat{\rho} = 0$ of DES has been characterized in a set membership framework, and it is shown that both space and time computational complexities in checking this property are polynomial in the cardinality of the set of states of the DES. Since, the conditions of [11] rely upon the set $\widehat{\mathcal{F}}$ and its complement (see Theorem 20), the generalization of such conditions to $(\widehat{\rho}, \widehat{\mathcal{F}})$ -diagnosability with $\widehat{\rho} \geq 0$ can simply be obtained by replacing the complement of $\widehat{\mathcal{F}}$ with the complement of $\widehat{\mathcal{B}}_{\widehat{\rho}}(\widehat{\mathcal{F}})$; obtained algorithms remain of polynomial computational complexity.

B. Main result

We start by defining a symbolic system that approximates Σ in the sense of approximate bisimulation for any desired accuracy. For convenience, we reformulate the nonlinear system Σ by using the formalism given in Definition 3.

Definition 6: Given Σ , define the system

$$S(\Sigma) = (X, X_0, U, \xrightarrow{\quad}, X_m, Y, H),$$

where

- $X = \mathbb{R}^n$;
- $X_0 = \mathcal{X}_0$;
- U coincides with the set U in (1);
- $x \xrightarrow{u} x^+$, if $x^+ = f(x, u)$;
- $Y = \mathbb{R}^p$;
- $H(x) = \begin{bmatrix} I_p & 0 \end{bmatrix} x$, for all $x \in X$.

System $S(\Sigma)$ is metric because set $X = \mathbb{R}^n$ can be equipped with a metric \mathbf{d} ; in the sequel we choose metric

$$\mathbf{d}(x, x') = \|x - x'\|, x, x' \in \mathbb{R}^n. \quad (8)$$

System $S(\Sigma)$ will be approximated by means of a system that we now introduce.

Definition 7: Given Σ , a state and output quantization parameter $\eta \in \mathbb{R}^+$ and an input quantization parameter $\mu \in \mathbb{R}^+$, define the system

$$S_{\eta, \mu}(\Sigma) = (X_{\eta, \mu}, X_{\eta, \mu, 0}, U_{\eta, \mu}, \xrightarrow{\eta, \mu}, Y_{\eta, \mu}, H_{\eta, \mu}),$$

where:

- $X_{\eta, \mu} = [\mathbb{R}^n]_{\eta}^n$;
- $X_{\eta, \mu, 0} = [\mathcal{X}_0]_{\eta}^n$;
- $U_{\eta, \mu} = [U]_{\mu}^m$;
- $\xi \xrightarrow{\eta, \mu} \xi^+$, if $\xi^+ = [f(\xi, v)]_{\eta}^n$;
- $Y_{\eta, \mu} = [\mathbb{R}^p]_{\eta}^p$;

- $H_{\eta,\mu}(\xi) = \begin{bmatrix} I_p & 0 \end{bmatrix} \xi$, for all $\xi \in X_{\eta,\mu}$.

The basic idea in the construction above is to replace each state x in Σ by its quantized value $\xi = [x]_{\eta}^n$ and each input $u \in U$ by its quantized value $v = [u]_{\mu}^m$ in $S_{\eta,\mu}(\Sigma)$. Accordingly, evolution of system Σ with initial state x and input v to state $x^+ = f(\xi, v)$, is captured by the transition $\xi \xrightarrow[\eta]{v} \xi^+$ in system $S_{\eta,\mu}(\Sigma)$, where ξ and ξ^+ are the quantized values of x and x^+ , respectively, i.e., $\xi = [x]_{\eta}^n$ and $\xi^+ = [x^+]_{\eta}^n$. System $S_{\eta,\mu}(\Sigma)$ is metric; in the sequel we use the metric \mathbf{d} in (8); this choice is allowed because $X_{\eta,\mu} \subset X$. Moreover, by definition of the transition relation $\xrightarrow[\eta,\mu]{v}$, system $S_{\eta,\mu}(\Sigma)$ is deterministic. By definition of $X_{\eta,\mu}$ and $U_{\eta,\mu}$, system $S_{\eta,\mu}(\Sigma)$ is countable. We now consider the following

Assumption 4: A locally Lipschitz function

$$V : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}_0^+$$

exists for nonlinear system Σ , which satisfies the following inequalities for some \mathcal{K}_{∞} functions $\underline{\alpha}$, $\bar{\alpha}$, λ and \mathcal{K} function σ :

- (i) $\underline{\alpha}(\|x - x'\|) \leq V(x, x') \leq \bar{\alpha}(\|x - x'\|)$, for any $x, x' \in \mathbb{R}^n$;
- (ii) $V(f(x, u), f(x', u')) - V(x, x') \leq -\lambda(V(x, x')) + \sigma(\|u - u'\|)$, for any $x, x' \in \mathbb{R}^n$ and any $u, u' \in U$.

Function V is called an incremental input-to-state stable (δ -ISS) Lyapunov function [29], [30] for nonlinear system Σ . Assumption 4 has been shown in [30] to be a sufficient condition for Σ to fulfill the δ -ISS stability property [29], [30].

We now have all the ingredients to present the following

Proposition 1: Suppose that Assumption 4 holds and let L be a Lipschitz constant of function V in $\mathbb{R}^n \times \mathbb{R}^n$. Then, for any desired accuracy $\varepsilon \in \mathbb{R}^+$ and for any quantization parameters $\eta, \mu \in \mathbb{R}^+$ satisfying the following inequalities

$$\begin{aligned} L\eta + \sigma(\mu) &\leq (\lambda \circ \underline{\alpha})(\varepsilon), \\ \bar{\alpha}(\eta) &\leq \underline{\alpha}(\varepsilon), \end{aligned} \quad (9)$$

relation $\mathcal{R}_{\varepsilon} \subseteq \mathbb{R}^n \times X_{\eta,\mu}$ specified by

$$(x, \xi) \in \mathcal{R}_{\varepsilon} \Leftrightarrow V(x, \xi) \leq \underline{\alpha}(\varepsilon) \quad (10)$$

is an ε -approximate bisimulation between $S(\Sigma)$ and $S_{\eta,\mu}(\Sigma)$. Consequently, systems $S(\Sigma)$ and $S_{\eta,\mu}(\Sigma)$ are ε -bisimilar.

Proof: Direct consequence of Proposition 1 in [31]. ■

We now show that under Assumption 4, system $S_{\eta,\mu}(\Sigma)$ is not only countable but also symbolic.

Proposition 2: Suppose that Assumption 4 holds. Then, for any quantization parameters $\eta, \mu \in \mathbb{R}^+$, system $S_{\eta,\mu}(\Sigma)$ is symbolic.

Proof: Under Assumption 4, the nonlinear system Σ is δ -ISS [30]. Given $\eta, \mu \in \mathbb{R}^+$, select $\varepsilon \in \mathbb{R}^+$ satisfying the inequality in (9). By Proposition 1, for any $t_f \in \mathbb{N}$ and for any state run

$$\xi(0) \xi(1) \dots \xi(t_f)$$

of $S_{\eta,\mu}(\Sigma)$ there exists a state trajectory $x : [0; t_f] \rightarrow \mathbb{R}^n$ of Σ such that:

$$(\xi(t), x(t)) \in \mathcal{R}_{\varepsilon}, \forall t \in [0; t_f].$$

By definition of $\mathcal{R}_{\varepsilon}$ in (10), the δ -ISS property and Assumption 1, we get for any $t \in [0; t_f]$ and for any $t_f \in \mathbb{N}$:

$$\begin{aligned} \|\xi(t)\| &\leq \|\xi(t) - x(t)\| + \|x(t)\| \\ &\leq \varepsilon + \beta(\|x(0)\|, t) + \gamma(\sup_{t' \in [0; t]} \|u(t')\|) \\ &\leq \varepsilon + \beta(\|x(0)\|, 0) + \gamma(\sup_{t' \in [0; t]} \|u(t')\|) \\ &\leq \varepsilon + \max_{x_0 \in \mathcal{X}_0} \beta(\|x(0)\|, 0) + \gamma(\max_{u \in U} \|u\|), \end{aligned}$$

for some \mathcal{KL} function β and \mathcal{K} function γ [30]. Hence,

$$\xi(t) \in \mathcal{B}_r(0), t \in \mathbb{N},$$

with $r = \varepsilon + \max_{x_0 \in \mathcal{X}_0} \beta(\|x(0)\|, 0) + \gamma(\max_{u \in U} \|u\|)$, and since $\xi(t) \in X_{\eta,\mu}$ for all $t \in \mathbb{N}$, we get

$$\text{Ac}(S_{\eta,\mu}(\Sigma)) \subseteq \mathcal{B}_r(0) \cap X_{\eta,\mu}$$

that is a finite set. Finally, since U is compact then $[U]_{\mu}^m$ is finite from which, the result follows. ■

Computational complexity in constructing $S_{\eta,\mu}(\Sigma)$ is discussed in the following

Proposition 3: Space and time computational complexities in computing $S_{\eta,\mu}(\Sigma)$ are exponential with the dimension n of state space and with the dimension m of the input space of Σ .

One way to mitigate computational complexity above is in constructing only the accessible part of $S_{\eta,\mu}(\Sigma)$; similar ideas were explored in [32] by following on-the-fly techniques studied in e.g. [33], [34] for efficient formal verification and control design of transition systems.

We now have all the ingredients to present the main result of this paper establishing connections between approximate diagnosability of $S_{\eta,\mu}(\Sigma)$ and approximate diagnosability of the original nonlinear system Σ .

Given a set $\mathcal{F} \subseteq \mathbb{R}^n$ and an accuracy $\varepsilon \in \mathbb{R}^+$, consider the sets

$$\begin{aligned} \mathcal{F}_{\varepsilon} &= \mathcal{B}_{\varepsilon}(\mathcal{F}) \cap [\mathbb{R}^n]_{\eta}^n, \\ \mathcal{F}'_{\varepsilon} &= \{x \in \mathcal{F} : \mathcal{B}_{\varepsilon}(x) \subseteq \mathcal{F}\} \cap [\mathbb{R}^n]_{\eta}^n. \end{aligned}$$

By construction above, we get:

$$\mathcal{F}'_{\varepsilon} \subseteq (\mathcal{F} \cap [\mathbb{R}^n]_{\eta}^n) \subseteq \mathcal{F}_{\varepsilon}.$$

Theorem 1: Consider nonlinear system Σ in (1) satisfying Assumption 4 and a set $\mathcal{F} \subseteq \mathbb{R}^n$. Consider a triplet $\varepsilon, \eta, \mu \in \mathbb{R}^+$ of parameters satisfying (9). The following statements hold:

- i) If $S_{\eta,\mu}(\Sigma)$ is $(k\eta, \mathcal{F}_{\varepsilon})$ -diagnosable, for some $k \in \mathbb{N}$, then Σ is (ρ, \mathcal{F}) -diagnosable, for any

$$\rho > 2\varepsilon + k\eta.$$

- ii) Suppose that set \mathcal{F} is with interior and parameter $\varepsilon \in \mathbb{R}^+$ is such that¹

$$\mathcal{F}'_{\varepsilon} \neq \emptyset. \quad (11)$$

¹Since \mathcal{F} is with interior there always exists $\varepsilon \in \mathbb{R}^+$ satisfying (11).

If Σ is (ρ, \mathcal{F}) -diagnosable, for some $\rho \in \mathbb{R}_0^+$, then $S_{\eta, \mu}(\Sigma)$ is $(k'\eta, \mathcal{F}'_\varepsilon)$ -diagnosable, for any integer

$$k' > \min\{h \in \mathbb{N} : (\rho + 2\varepsilon) \leq h\eta\}.$$

Proof: (Proof of i.) By contradiction, suppose that $S_{\eta, \mu}(\Sigma)$ is $(k\eta, \mathcal{F}_\varepsilon)$ -diagnosable, but Σ is not (ρ, \mathcal{F}) -diagnosable, with $\rho > 2\varepsilon + k\eta$. Then $\forall \Delta \in \mathbb{N}$ there exists a state trajectory x^f of Σ such that for some $\mathbf{t} > 0$

$$(x^f(\mathbf{t}) \in \mathcal{F}) \wedge (x(t) \notin \mathcal{F}, \forall t \in [0; \mathbf{t} - 1])$$

and a state trajectory x^s of Σ such that

$$\mathcal{B}_\rho(x^s(t)) \cap \mathcal{F} = \emptyset, \forall t \in [0; \mathbf{t} + \Delta] \quad (12)$$

and, by denoting by $y_{\mathbf{t}+\Delta, \eta}^f$ and $y_{\mathbf{t}+\Delta, \eta}^s$ the quantized output trajectories associated to $x^f|_{[0; \mathbf{t}+\Delta]}$ and to $x^s|_{[0; \mathbf{t}+\Delta]}$, respectively, we have

$$y_{\mathbf{t}+\Delta, \eta}^f = y_{\mathbf{t}+\Delta, \eta}^s.$$

Since $S(\Sigma) \cong_\varepsilon S_{\eta, \mu}(\Sigma)$, for any state trajectory x of Σ there exists a state run $\xi(0) \xi(1) \dots$ of $S_{\eta, \mu}(\Sigma)$, such that

$$\|\xi(t) - x(t)\| \leq \varepsilon, \forall t \in \mathbb{N}$$

By construction of \mathcal{F}_ε , if $x^f(\mathbf{t}) \in \mathcal{F}$ then

$$\mathcal{B}_\varepsilon(x^f(\mathbf{t})) \cap [\mathbb{R}^n]_\eta^n \subseteq \mathcal{F}_\varepsilon.$$

Moreover, since $\rho > 2\varepsilon + k\eta$ and condition (12) holds, then

$$\mathcal{B}_{\varepsilon+k\eta}(x^s(t)) \cap \mathcal{F}_\varepsilon = \emptyset.$$

Therefore $\forall \Delta \in \mathbb{N}$ there exist two state runs $\xi'(0) \xi'(1) \dots$ and $\xi''(0) \xi''(1) \dots$ of $S_{\eta, \mu}(\Sigma)$, the first one such that for some $\mathbf{t}' \in [0; \mathbf{t}]$

$$(\xi'(\mathbf{t}') \in \mathcal{F}_\varepsilon) \wedge ((\mathbf{t}' = 0) \vee (\xi'(t) \notin \mathcal{F}_\varepsilon, \forall t \in [0; \mathbf{t}' - 1]))$$

and the other one such that

$$\xi''(t) \notin \mathcal{B}_{k\eta}(\mathcal{F}_\varepsilon), \forall t \in [0; \mathbf{t}' + \Delta]$$

with the same corresponding output runs, i.e.

$$y_{\mathbf{t}+\Delta, \eta}' = y_{\mathbf{t}+\Delta, \eta}''$$

Therefore $S_{\eta, \mu}(\Sigma)$ is not $(k\eta, \mathcal{F}_\varepsilon)$ -diagnosable, and the first statement follows.

(Proof of ii.) Again by contradiction, suppose that Σ is (ρ, \mathcal{F}) -diagnosable, but $S_{\eta, \mu}(\Sigma)$ is not $(k'\eta, \mathcal{F}'_\varepsilon)$ -diagnosable, with ε, η, μ satisfying (9), ε such that $\mathcal{F}'_\varepsilon \neq \emptyset$, and $k' > \min_{h \in \mathbb{N}} h\eta : (\rho + 2\varepsilon) \leq h\eta$. Then $\forall \Delta \in \mathbb{N}$ there exists a state run ξ^f of $S_{\eta, \mu}(\Sigma)$ such that for some $\mathbf{t} > 0$

$$(\xi^f(\mathbf{t}) \in \mathcal{F}'_\varepsilon) \wedge (x(t) \notin \mathcal{F}'_\varepsilon, \forall t \in [0; \mathbf{t} - 1])$$

and a state run ξ^s of $S_{\eta, \mu}(\Sigma)$ such that

$$\mathcal{B}_{k'\eta}(\xi^s(t)) \cap \mathcal{F}'_\varepsilon = \emptyset, \forall t \in [0; \mathbf{t} + \Delta] \quad (13)$$

and, by denoting with $y_{\mathbf{t}+\Delta, \eta}^f$ and $y_{\mathbf{t}+\Delta, \eta}^s$ the output runs associated to $\xi^f|_{[0; \mathbf{t}+\Delta]}$ and to $\xi^s|_{[0; \mathbf{t}+\Delta]}$, respectively, we have

$$y_{\mathbf{t}+\Delta, \eta}^f = y_{\mathbf{t}+\Delta, \eta}^s.$$

Since $S(\Sigma) \cong_\varepsilon S_{\eta, \mu}(\Sigma)$, for any state run $\xi(0) \xi(1) \dots$ of $S_{\eta, \mu}(\Sigma)$ there exists a state trajectory x of Σ , such that

$$\|\xi(t) - x(t)\| \leq \varepsilon, \forall t \in \mathbb{N}.$$

By construction of \mathcal{F}'_ε , if $\xi^f(\mathbf{t}) \in \mathcal{F}'_\varepsilon$ then

$$\mathcal{B}_\varepsilon(\xi^f(\mathbf{t})) \subseteq \mathcal{F}.$$

Moreover, since $k' > \min_{h \in \mathbb{N}} h\eta : (\rho + 2\varepsilon) \leq h\eta$, and since condition (13) holds, then $\mathcal{B}_{k'\eta}(\xi^s(t)) \cap \mathcal{F} = \emptyset$. Therefore $\forall \Delta \in \mathbb{N}$ there exist two state trajectories x' and x'' of Σ , the first one such that for some $\mathbf{t}' \in [0; \mathbf{t}]$

$$(x'(\mathbf{t}') \in \mathcal{F}) \wedge (x'(t) \notin \mathcal{F}, \forall t \in [0; \mathbf{t}' - 1])$$

and the other one such that

$$x''(t) \notin \mathcal{B}_{k'\eta}(\mathcal{F}), \forall t \in [0; \mathbf{t}' + \Delta]$$

with the same corresponding quantized output trajectories, i.e.

$$y_{\mathbf{t}+\Delta, \eta}' = y_{\mathbf{t}+\Delta, \eta}''$$

Therefore Σ is not $(k'\eta, \mathcal{F})$ -diagnosable. Since $k'\eta > (\rho + 2\varepsilon)$, then $k'\eta > \rho$, Σ is not (ρ, \mathcal{F}) -diagnosable and the proof is complete. ■

Remark 4: While statement i) of Theorem 1 is useful to check if Σ is (ρ, \mathcal{F}) -diagnosable, statement ii) can be used in its logical negation form as a tool to check if Σ is not (ρ, \mathcal{F}) -diagnosable.

We conclude this section with a computational complexity analysis of the approach proposed. By combining Remark 3 and Proposition 3 we get

Theorem 2: Space and time computational complexities in checking (ρ, \mathcal{F}) -diagnosability of Σ are exponential with the dimension n of state space and with the dimension m of the input space of Σ .

V. CONCLUSIONS

In this paper we proposed a novel notion of diagnosability, termed approximate diagnosability, for discrete-time nonlinear systems with unknown inputs and quantized output measurements. Under an assumption of incremental stability of the nonlinear system we first derived a symbolic model. We extended the classical notion of diagnosability given for DES to metric symbolic systems. We then established the relation between approximate diagnosability of the nonlinear system and approximate diagnosability of the symbolic model. Computational complexity of the approach taken is also discussed.

REFERENCES

- [1] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 40, no. 9, pp. 1555–1575, 1995.
- [2] W. Wang, S. Lafortune, A. Girard, and F. Lin, "Optimal sensor activation for diagnosing discrete event systems," *Automatica*, vol. 46, pp. 1165–1175, 2010.
- [3] W. Wang, A. Girard, S. Lafortune, and F. Lin, "On codiagnosability and coobservability with dynamic observations," *IEEE Transactions on Automatic Control*, vol. 56, no. 7, pp. 1551–1566, 2011.

- [4] R. Debouk, R. Malik, and B. Brandin, "A modular architecture for diagnosis of discrete event systems," in *Proceedings of the 41th Conference on Decision and Control, Las Vegas, Nevada, USA*, December 2002, pp. 417–422.
- [5] R. Su and W. Wonham, "Global and local consistencies in distributed fault diagnosis for discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 50(12), pp. 1923–1935, 2005.
- [6] C. Zhou, R. Kumar, and R. S. Sreenivas, "Decentralized modular diagnosis of concurrent discrete event systems," in *Proceedings of the 9th International Workshop on Discrete Event Systems Gteborg, Sweden*, May 2008, pp. 28–30.
- [7] K. W. Schmidt, "Verification of modular diagnosability with local specifications for discrete-event systems," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 43(5), pp. 1130–1140, 2013.
- [8] S. Zad, R. Kwong, and W. Wonham, "Fault diagnosis in discrete-event systems: Framework and model reduction," *IEEE Transactions on Automatic Control*, vol. 48, no. 7, pp. 51–65, July 2003.
- [9] S. Ricker and J. van Schuppen, "Decentralized failure diagnosis with asynchronous communication between diagnosers," in *Proceedings of the European Control Conference*, Porto, Portugal, 2001.
- [10] J. Zaytoon and S. Lafortune, "Overview of fault diagnosis methods for discrete event systems," *Annual Reviews in Control*, vol. 37, no. 2, pp. 308–320, 2013.
- [11] E. De Santis and M.D. Di Benedetto, "Observability and diagnosability of finite state systems: a unifying framework," *Automatica*, 2017, to Appear. Available online at arXiv:1608.03195 [math.OC].
- [12] R. Stengel, "Intelligent failure-tolerant control," *IEEE Control Systems Magazine*, vol. 11, pp. 14–23, June 1991.
- [13] M. Blanke, R. Izadi-Zamanabadi, S. Bogh, and C. Lunau, "Fault-tolerant control systems – a holistic view," *Control Engineering Practice*, vol. 5, pp. 693–702, May 1997.
- [14] R. Patton, "Fault-tolerant control systems: The 1997 situation," in *Proc. IFAC Symp. Fault Detect., Supervision Safety Techn. Process*, 1997, pp. 1033–1054.
- [15] J. Jiang, "Fault-tolerant control systems – an introductory overview," *Acta Autom. Sinica*, vol. 31, pp. 161–174, January 2005.
- [16] J. Lunze and J. Richter, "Reconfigurable fault-tolerant control: A tutorial introduction," *European Journal of Control*, vol. 144, pp. 359–386, 2008.
- [17] Y. Zhang and J. Jiang, "Bibliographical review and reconfigurable fault-tolerant control systems," *Annual Reviews in Control*, vol. 32, pp. 229–252, December 2008.
- [18] M. Benosman, "A survey of some recent results on nonlinear fault tolerant control," *Math. Probl. Eng.*, vol. 2010, 2010.
- [19] Z. Gao, C. Cecati, and S. Ding, "A survey of fault diagnosis and fault-tolerant techniques—part i: Fault diagnosis with model-based and signal-based approaches," *IEEE Transactions on Industrial Electronics*, vol. 62, pp. 3757–3767, June 2015.
- [20] S. Tripakis, "Fault diagnosis for timed automata," in *Formal Techniques in Real-Time and Fault-Tolerant Systems*, ser. Lecture Notes in Computer Science. Berlin: Springer Verlag, 2002, pp. 205–221.
- [21] M. Bayouduh, L. Travé-Massuyes, X. Olive, and T. A. Space, "Hybrid systems diagnosis by coupling continuous and discrete event techniques," in *Proc. IFAC World Congress*, 2008, pp. 7265–7270.
- [22] M. Bayouduh, L. Travé-Massuyes, and X. Olive, "Hybrid systems diagnosability by abstracting faulty continuous dynamics," in *Proc. 17th Int. Principles Diagnosis Workshop*, 2006, pp. 9–15.
- [23] M. D. Di Benedetto, S. Di Gennaro, and A. D’Innocenzo, "Verification of hybrid automata diagnosability by abstraction," *IEEE Transactions on Automatic Control*, vol. 56, pp. 2050–2061, 2011.
- [24] Y. Deng, A. D’Innocenzo, M. D. Di Benedetto, S. Di Gennaro, and A. Julius, "Verification of hybrid automata diagnosability with measurement uncertainty," *IEEE Transactions on Automatic Control*, vol. 61, pp. 982–993, 2016.
- [25] J. Lunze, "Diagnosis of quantized systems based on a timed discrete-event model," *IEEE Transactions on Man and Cybernetics – Part A: Systems and Humans*, vol. 30, pp. 322–335, May 2000.
- [26] C. De Persis, "Detecting faults from encoded information," in *Proc. of the 42nd IEEE Conference on Decision and Control*, 2013, pp. 947–952.
- [27] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer, 2009.
- [28] A. Girard and G. Pappas, "Approximation metrics for discrete and continuous systems," *IEEE Transactions on Automatic Control*, vol. 52, no. 5, pp. 782–798, 2007.
- [29] D. Angeli, "A Lyapunov approach to incremental stability properties," *IEEE Transactions on Automatic Control*, vol. 47, no. 3, pp. 410–421, 2002.
- [30] B. Bayer, M. Burger, and F. Allgower, "Discrete-time incremental ISS: A framework for robust NMPS," in *European Control Conference*, Zurich, Switzerland, July 2013, pp. 2068–2073.
- [31] G. Pola, P. Pepe, and M.D. Di Benedetto, "Symbolic models for networks of control systems," *IEEE Transactions on Automatic Control*, vol. 61, no. 11, pp. 3663–3668, November 2016.
- [32] G. Pola, A. Borri, and M. D. Di Benedetto, "Integrated design of symbolic controllers for nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 57, no. 2, pp. 534–539, feb. 2012.
- [33] C. Courcoubetis, M. Vardi, P. Wolper, and M. Yannakakis, "Memory-efficient algorithms for the verification of temporal properties," *Formal Methods in System Design*, vol. 1, no. 2-3, pp. 275–288, 1992.
- [34] S. Tripakis and K. Altisen, "On-the-fly controller synthesis for discrete and dense-time systems," in *World Congress on Formal Methods in the Development of Computing Systems*, ser. Lecture Notes in Computer Science. Berlin: Springer Verlag, September 1999, vol. 1708, pp. 233 – 252.